

ALEX G. TSE (CABN 152348)  
Acting United States Attorney

BARBARA J. VALLIERE (DCBN 439353)  
Chief, Criminal Division

JULIE D. GARCIA (CABN 288624)  
Assistant United States Attorney

450 Golden Gate Avenue, Box 36055  
San Francisco, California 94102-3495  
Telephone: (415) 436-6758  
FAX: (415) 436-7234  
Julie.Garcia@usdoj.gov

**FILED**

MAY - 2 2018

Attorneys for United States of America

SUSAN Y. SOONG  
CLERK, U.S. DISTRICT COURT  
NORTHERN DISTRICT OF CALIFORNIA

UNITED STATES DISTRICT COURT  
FOR THE NORTHERN DISTRICT OF CALIFORNIA  
SAN FRANCISCO DIVISION

IN THE MATTER OF THE SEARCH OF  
A RESIDENCE IN APTOS,  
CALIFORNIA 95003

No. 17-70656 JSC

DECLARATION OF DANIEL COSTIN IN  
SUPPORT OF APPLICATION FOR TIME  
EXTENSION

I, Daniel Costin, hereby declare:

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI") and have been employed by the FBI as such since January 2008. I am currently assigned to the squad that investigates Child Exploitation matters in the San Francisco Division's Oakland Resident Agency. I am a trained Digital Evidence Extraction Technician (DEXT), which authorizes me to search, find, and extract digital evidence in support of FBI investigations. As part of my duties as an FBI agent, I investigate criminal violations relating to child exploitation and child pornography, including violations pertaining to the

DECLARATION OF DANIEL COSTIN IN SUPPORT OF APPLICATION FOR TIME EXTENSION  
CR No. 17-70656 JSC

1 illegal production, distribution, receipt, and possession of child pornography, in violation of 18 U.S.C.  
2 §§ 2251, 2252, and 2252A.

3 2. This declaration is made in support of a request for an order providing the government additional  
4 time to retain and forensically image, index, and search certain items that were seized pursuant to the  
5 search warrant issued in the above-captioned matter.

6 3. On April 26, 2017, the Honorable Jacqueline Scott Corley, United States Magistrate Judge for  
7 the Northern District of California, signed a search warrant for a residence in Aptos, California (the  
8 "Residence"), including computer equipment and electronic storage media therein. The purpose of the  
9 Search Warrant, which is attached as **Exhibit A** to this Declaration, was to seize and search for items  
10 constituting evidence, contraband, fruits, or instrumentalities relating to violations of 18 U.S.C.  
11 § 2252(a)(2) and 2252(a)(4)(B), which prohibit the receipt, distribution and possession of child  
12 pornography. The search authorized by the warrant was executed on April 27, 2017, and the following  
13 electronic media items were seized:

- 14 1. Black Apple iPhone 7, Model A1660, S/N F72SDRNGHG71
- 15 2. Western Digital MyPassport External Hard Drive, S/N WX91A10C0217
- 16 3. Black and green Transcend 1TB Portable Hard Drive, S/N C842472715
- 17 4. Black Sabrent Portable Hard Drive, no serial number
- 18 5. Black Apple iWatch
- 19 6. Black Motorola Cellular Phone
- 20 7. Black and silver 8GB Apple iPod
- 21 8. Black Apple 64GB iPad, Model A1416, S/N DLXH3A4JDJ8V
- 22 9. White and silver Apple Mac Mini, S/N YM7467LVYL1
- 23 10. Black Lenovo Laptop, Model WB0109290E, S/N WB03435432
- 24 11. Alienware Laptop, Model P42F, S/N 451PM32
- 25 12. Black Amcrest 1080P Wireless IP Camera, Model IP2M-841B, S/N  
26 AMC0007X137X70D028 with 32GB SanDisk Memory Card

27 4. These items were seized because, due to the large volume of electronic evidence found on-site,  
28

1 it was determined the digital items could not be imaged and searched on-site in any practical manner.  
2 Attachment C to the Search Warrant, which sets forth this District's protocol for the seizure and  
3 searching of electronic items, authorized agents to image the evidence within 60 days and to search it  
4 within 120 days. Attachment C further provided in Paragraph 7 that "[t]he time period set forth in this  
5 protocol may be extended by court order for good cause."

6 5. The review of the Apple iPhone 7, the Motorola cell phone, and the Alienware laptop indicated  
7 that all three devices contain child pornography. Because these items contain illegal contraband and  
8 evidence of the crimes being investigated, they will not be returned to their owner.

9 6. Five of the devices—the iWatch, the iPod, the iPad, the Mac Mini, and the wireless camera—  
10 have been imaged and reviewed and do not contain child pornography. The black Lenovo laptop was  
11 missing a hard drive and did not contain child pornography either.

12 7. Five of the devices, two of which have already been determined to contain child pornography,  
13 are entirely or partially encrypted, specifically:

- 14 1. Black Apple iPhone 7, Model A1660, S/N F72SDRNGHG71
- 15 2. Western Digital MyPassport External Hard Drive, S/N WX91A10C0217
- 16 3. Black and green Transcend 1TB Portable Hard Drive, S/N C842472715
- 17 4. Black Sabrent Portable Hard Drive, no serial number
- 18 5. Alienware Laptop, Model P42F, S/N 451PM32

19 Due to the encryption, the FBI has thus far been unable to fully access or review all of the contents of  
20 these devices.

21 8. On August 10, 2017, the Honorable Elizabeth D. Laporte, United States Magistrate Judge for the  
22 Northern District of California, signed an Order, attached as **Exhibit B** to this Declaration, authorizing  
23 retention of these electronic devices for an additional 120 days.

24 9. On December 11, 2017, Judge Laporte signed another Order, attached as **Exhibit C** to this  
25 Declaration, authorizing retention of these electronic devices for an additional 120 days.

26 10. On April 26, 2018, the Honorable United States District Court Judge Charles R. Breyer issued an  
27 order requiring the devices' owner to decrypt and/or unlock the encrypted and/or password-protected  
28

1 portions of the black iPhone 7, the Transcend 1TB hard drive, and the Alienware laptop. *See* CR 17-259  
2 CRB-2, Dkt. 83.

3 11. Based on my training and experience, I anticipate that, once the defendant has decrypted the  
4 three devices at issue in the decryption order, evidence on those devices may assist the FBI in  
5 determining the passwords for the remaining two devices, thereby permitting the FBI to access and  
6 review their contents.

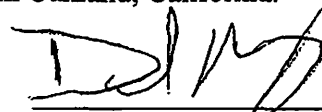
7 12. This declaration is offered to demonstrate the good cause that supports an order providing the  
8 FBI with additional time to decrypt, access, review, and complete the forensic processing of the  
9 aforementioned items. Attempting to access, processing, and reviewing encrypted electronic evidence is  
10 a labor-intensive process that must be performed by an individual trained in forensically sound digital  
11 evidence extraction techniques. In this case, the imaging of and attempt to access the five encrypted  
12 devices took time and resources away from the processing and review of other devices.

13 13. Additional time is also warranted in this case because of the evidence found to date—that is,  
14 illegal contraband and evidence of violations of 18 U.S.C. § 2252(a)(2) and 2252(a)(4)(B)—and to  
15 assure that the devices not yet imaged or searched do not contain additional contraband and/or evidence  
16 of the crimes being investigated.

17 14. For these reasons the FBI seeks an additional 120 days total to review the devices referenced in  
18 paragraph 2 for evidence of the crimes being investigated, consistent with the scope of the search  
19 warrant issued on April 26, 2017, and the extensions issued by the Court on August 10, 2017, and  
20 December 11, 2017.

21 I declare under penalty of perjury that the foregoing is true and correct to the best of my  
22 knowledge.

23 Executed on this 1st day of May, 2018, in Oakland, California.

24   
25 \_\_\_\_\_  
26 Special Agent Daniel Costin  
27 Federal Bureau of Investigation  
28

# EXHIBIT A

AO 93 (Rev. 12/09) Search and Seizure Warrant

**UNDERSEAL****UNITED STATES DISTRICT COURT**for the  
Northern District of California**JSC**In the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address))  
)  
) Case No.  
)  
)  
)**3-17-70656****SEARCH AND SEIZURE WARRANT**

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Northern District of California  
(Identify the person or describe the property to be searched and give its location):

See Attachment A.

The person or property to be searched, described above, is believed to conceal (Identify the person or describe the property to be seized):

See Attachment B.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property.

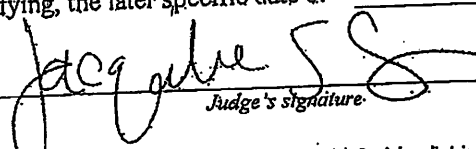
YOU ARE COMMANDED to execute this warrant on or before

May 10, 2017  
(not to exceed 14 days)☒ in the daytime 6:00 a.m. to 10 p.m.☐ at any time in the day or night as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to United States Magistrate Judge  
Hon. Jacqueline Scott Corley  
(name)☐ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box) ☐ for \_\_\_\_\_ days (not to exceed 30).  
☐ until, the facts justifying, the later specific date of \_\_\_\_\_

Date and time issued:

4/26/17 7:50 p.m.  
Judge's signatureCity and state: San Francisco, CaliforniaHon. Jacqueline Scott Corley, U.S. Magistrate Judge  
Printed name and title

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
-----------	---------------------------------	--

Inventory made in the presence of:

Inventory of the property taken and name of any person(s) seized:

### Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: \_\_\_\_\_

Executing officer's signature

Printed name and title

ATTACHMENT A

Description of Property to Be Searched

1. The SUBJECT PREMISES at [REDACTED] is a tan colored two story residential structure with a brown door on the west side of the residence. Affixed to the right hand side of the door are three white numbers hung vertically [REDACTED]. The residence has two garages, one attached to the residence and one detached on the north-west side of the residence. The two garages are connected by a black steel gate. Both garages have grey doors. In the rear of the property is a brown shed with white trim.

The premises to be searched includes all rooms, attics, closed containers, and other places therein, any appurtenances to the real property that is the SUBJECT PREMISES of [REDACTED] and any associated storage areas.

This warrant includes the search of the person of Ryan Michael Spencer, date of birth [REDACTED]



**ATTACHMENT B**

**Description of Particular Things to be Seized**

The following materials, which constitute contraband, evidence, instrumentalities, or fruits of violations of 18 U.S.C. §§ 2252(a)(2) and 2252(a)(4)(B), which prohibit the receipt, distribution and possession of child pornography:

1. Computers or storage media used as a means to:
  - a. visually depict minors engaged in sexually explicit conduct;
  - b. contain information pertaining to a sexual interest in children or in child pornography;
  - c. distribute, receive, or possess child pornography; or
  - d. communicate with or about minors engaged in sexually explicit conduct.
2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):
  - a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat", instant messaging logs, photographs, and correspondence;
  - b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software; as well as evidence of the presence or absence of security software designed to detect malicious software;

- c. evidence of the lack of such malicious software;
- d. evidence indicating how and when the COMPUTER was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the COMPUTER user;
- e. evidence indicating the COMPUTER user's state of mind as it relates to the crime under investigation;
- f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- h. evidence of the times the COMPUTER was used;
- i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- k. evidence about Internet Protocol addresses used by the COMPUTER;
- l. evidence about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
- m. evidence containing key-word search terms related to child pornography or references to websites related to child pornography; and

n. contextual information necessary to understand the evidence described in this attachment.

3. Routers, modems, and network equipment used to connect computers to the Internet.

4. Child pornography and child erotica.

5. Records, information, and items relating to violations of the statutes described above including:

- a. Records, information, and items relating to the occupancy or ownership of [REDACTED] [REDACTED] including utility and telephone bills, mail envelopes, or addressed correspondence; Records, information, and items relating to the ownership or use of computer equipment found in the above residence, including sales receipts, bills for Internet access, and handwritten notes;
- b. Records and information relating to the identity or location of the persons suspected of violating the statutes described above; and
- c. Records and information relating to sexual exploitation of children.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions,

including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

ATTACHMENT C

December 10, 2010, United States District Court for the Northern District of California

PROTOCOL FOR SEARCHING DEVICES OR MEDIA THAT STORE DATA  
ELECTRONICALLY

THIS PROTOCOL WILL BE ATTACHED TO EACH SEARCH WARRANT THAT  
AUTHORIZES A SEARCH OF ANY DEVICE OR MEDIA THAT STORES DATA  
ELECTRONICALLY

1. In executing this warrant, the government will begin by ascertaining whether all or part of a search of a device or media that stores data electronically ("the device") reasonably can be completed at the location listed in the warrant ("the site") within a reasonable time. If the search reasonably can be completed on-site, the government will remove the device from the site only if removal is necessary to preserve evidence, or if the item is contraband, a forfeitable instrumentality of the crime, or the fruit of a crime.
2. If the government determines that a search reasonably cannot be completed on site within a reasonable time period, the government must determine whether all or part of the authorized search can be completed by making a mirror image of, or in some other manner duplicating, the contents of the device and then conducting the forensic review of the mirror image or duplication off site. The government will complete a forensic review of that mirror image within 120 days of the execution of the search warrant.
3. In a circumstance where the government determines that a mirror image of the contents of a device cannot be created on site in a reasonable time, the government may seize and retain that device for 60 days in order to make a mirror image of the contents of the device.
4. When the government removes a device from the searched premises it may also remove any equipment or documents ("related equipment or documents") that reasonably appear to be necessary to create a mirror image of the contents of the device or conduct an off-site forensic review of a device.
5. When the government removes a device or related equipment or documents from the site in order to create a mirror image of the device's contents or to conduct an off-site forensic review of the device, the government must file a return with a magistrate judge that identifies with particularity the removed device or related equipment or documents within 14 calendar days of the execution of the search warrant.
6. Within a reasonable period of time, but not to exceed 60 calendar days after completing the forensic review of the device or image, the government must use reasonable efforts to return, delete, or destroy any data outside the scope of the warrant unless the government is otherwise permitted by law to retain such data.
7. The time periods set forth in this protocol may be extended by court order for good cause.

8. In the forensic review of any device or image under this warrant the government must make reasonable efforts to use methods and procedures that will locate and expose those categories of files, documents, or other electronically-stored information that are identified with particularity in the warrant, while minimizing exposure or examination of irrelevant, privileged, or confidential files to the extent reasonably practicable.

9. For the purposes of this search protocol, the phrase "to preserve evidence" is meant to encompass reasonable measures to ensure the integrity of information responsive to the warrant and the methods used to locate same.

# **EXHIBIT B**

UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF CALIFORNIA  
SAN FRANCISCO DIVISION

IN THE MATTER OF THE SEARCH OF )  
A RESIDENCE IN APTOS, )  
CALIFORNIA 95003 )

CASE NO. 17-70656 JSC

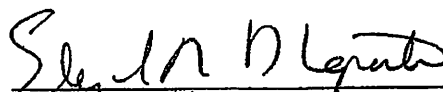
[PROPOSED] ORDER AUTHORIZING  
RETENTION OF ELECTRONIC DEVICES  
FOR AN ADDITIONAL 120 DAYS

Upon application of the United States of America and good cause appearing,

IT IS HEREBY ORDERED that the deadlines set forth in Paragraph 2, Paragraph 3, and Paragraph 6 of Attachment C of the search warrant in this matter authorized on April 26, 2017, be and hereby are extended by an additional 120 days.

IT IS SO ORDERED.

DATED: August 11, 2017

  
HON. ELIZABETH D. LAPORTE  
United States Magistrate Judge

[PROPOSED] ORDER AUTHORIZING RETENTION OF ELECTRONIC DEVICES FOR ADDITIONAL 120 DAYS  
No. 17-70656 JSC

# **EXHIBIT C**

**[PROPOSED] ORDER AUTHORIZING  
RETENTION OF ELECTRONIC DEVICES  
FOR AN ADDITIONAL 120 DAYS**